DOT Rules of Behavior

April, 2014

Version 4

Background

The Office of Management and Budget (OMB) Circular A-130, Appendix III, paragraph 3 (2)(a) requires that all Federal agencies promulgate rules of behavior that "clearly delineate responsibilities and expected behavior of all individuals with access" to the agencies' information and information systems, as well as state clearly the "consequences of behavior not consistent" with the rules of behavior. Additionally OMB M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information, requires agencies to promulgate "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance." The Rules of Behavior that follow are required to be used throughout DOT.

Congress and OMB require the promulgation of government-wide rules of behavior for two reasons. First, Congress and OMB recognize that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computers and the DOT data they contain or that may be accessed through their computers, in addition to the protection of DOT information in any form (e.g. digital, paper), are essential aspects of their jobs. Second, individuals must be held accountable for their use of DOT information and information systems.

Since written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using "due diligence" and the highest ethical standards to guide their actions. Personnel must understand that these rules are based on federal laws, OMB and other guidance, and DOT policies.

Applicability

The DOT Rules of Behavior address notice and consent issues identified by the Department of Justice and other sources. These rules also serve to clarify the roles of agency management and information system administrators, and serve to provide notice of what is considered acceptable use of all DOT information and information systems and acceptable behavior of DOT users. (Exception: These Rules of Behavior do not apply to members of the public accessing publically available DOT information systems.)

The following Rules of Behavior apply to all Department of Transportation (DOT) employees as well as contractor personnel that use or access DOT systems and Information Technology (IT) resources such

as workstations, laptop computers and portable electronic devices (PED) to access, store, receive, or transmit sensitive information.[1] PEDs include personal digital assistants or PDAs (e.g., Palm Pilots), cell phones, text messaging systems (e.g., BlackBerry), and plug-in and wireless peripherals that employ removable media (e.g., CDs, DVDs). PEDs also encompass USB flash memory (thumb) drives, external drives, and diskettes.

These Rules of Behavior are consistent with IT security policy in DOT Order 1351.37 Departmental Cybersecurity Policy and its associated Departmental Cybersecurity Compendium, as well as DOT Order 1351.33 Departmental Web-based Interactive Technologies Policy (Social Media and Web 2.0) and its Appendix A: Employee Conduct Policy. The Rules of Behavior apply to users at their primary workplace and at any alternative workplaces (e.g., telecommuting from home or from a satellite site). They also apply to users on travel when using DOT-issued information technology or when accessing DOT information systems when on travel.

The DOT Rules of Behavior must be acknowledged annually by all DOT federal employees, contractors, and other personnel who are provided access to DOT information or to DOT information systems. The Office of the DOT Chief Information Officer (DOT OCIO) makes these Rules of Behavior available via the DOT online training management systems (TMS) for employees and the DOT Security Awareness Training (SAT) application for its contractors. Users are encouraged to complete the online Rules of Behavior training and signify their acknowledgment via the training system. Otherwise, the Rules of Behavior must be printed and signed with a copy provided to the Information Systems Security Manager (ISSM) and the Privacy Officer of the employing DOT Component.

DOT Components are responsible for developing any system-specific Rules of Behavior needed to complement the General Rules of Behavior. Any such Rules of Behavior will also require user acknowledgement by way of signature.

General Rules of Behavior for Users of DOT Systems and IT Resources that

Access, Store, Receive, or Transmit DOT Information

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, DOT owned or controlled information systems, sensitive information, including Personally Identifiable Information (PII)[2], or information systems of the U.S. Department of Transportation.

---

[1] ***Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.***

2 PII is any information about a human being, living or deceased, regardless of nationality, that is maintained by an agency and that is linked or linkable to an individual and permits identification of that individual to be reasonably inferred by either direct or indirect means (e.g., data mining).

1 System Access

a) I understand that I must complete mandatory periodic (at least annual) security and privacy awareness training within designated timeframes and must complete any additional system-specific required training for the particular systems to which I require access.

b) I understand that I have no expectation of privacy while using any DOT equipment or while using DOT internet or e-mail services.

c) I understand that I will only be given access to those systems for which I require access to perform my official duties.

d) I will not attempt to access systems or information I am not authorized to access.

e) I will be presented with the System Use Notification Banner below and be required to acknowledge it prior to access to DOT information systems:
"You are accessing a U.S. Government information system, which includes this computer, the computer network on which it is connected, all other computers connected to this network, and all storage media connected to this computer or other computers on this network. This information system is provided for U.S Government use only. Unauthorized or improper use of this information may result in disciplinary action, as well as civil and criminal penalties. By using this information system you consent to the following:

   i. You have no reasonable expectation of privacy regarding any communications or data transiting this network or stored in this information system.

   ii. At any time, and for any lawful government purpose, the government may monitor, intercept, search and seize any communication or data transiting or stored on this information system.

   iii. Any communication or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

2 2 Passwords and Other Access Control Measures

a) I will choose passwords that are at least twelve characters long and have a combination of letters (upper- and lower-case), numbers, and special characters (Note: DOT systems will enforce this requirement in different ways and patterns of characters).

b) I will protect passwords, PINs and access numbers from disclosure. I will not share passwords. I will not provide my password to anyone, including system administrators. I will not record passwords or access control numbers on paper or in electronic form and store them on or with DOT workstations, laptop computers, or PEDs. To prevent others from obtaining my password by looking over my shoulder, I will shield my keyboard from view as I enter my password.

c) I will not leave smart cards unattended, on or with DOT workstations, laptop computers, or PEDs.

d) I will promptly change a password whenever I suspect my password has been compromised.

e) I will not attempt to bypass access control measures.

3 Data Access and Protection

a) I understand that I am permitted to access DOT information systems and networks from DOT-provided office equipment (e.g., workstations, laptops, PEDs).

b) I will not use personally-owned equipment to access DOT information systems and networks or process DOT information unless I am given expressed written approval from the system Authorizing Official, Component ISSM, or Component CIO. If I am granted permission to use personally-owned equipment for access to DOT information systems or networks:

   i. I agree to allow authorized DOT personnel to examine the personal IT device(s) that I have been granted permission to use, whether remotely or in any setting, so long as the personal devices are used to access or process DOT information.

   ii. I agree to use DOT-approved encryption, virus protection software, anti-spyware, and firewall/intrusion detection software and ensure the software is configured to meet DOT configuration requirements prior to connection to DOT networks. Verification of configuration is performed by Component CIO office.

   iii. I will use DOT-provided encryption to encrypt any e-mail, including attachments to the e-mail, which contains DOT sensitive information or PII before sending the email. I will not send any e-mail that contains DOT sensitive information in an unencrypted form. DOT sensitive information includes Personally Identifiable Information (PII).

   iv. I will not store or transport any DOT sensitive information on any portable storage media or device unless it is encrypted using DOT-approved encryption.

v. As DOT progresses with the deployment of Personal Identity Verification (PIV) cards for DOT personnel and subsequently DOT systems are capable of accepting PIV cards for user logins, I will use the PIV card issued to me for access to these systems as directed by the system owner.

c) I will protect sensitive information including PII from disclosure to unauthorized persons or groups.

d) I will ensure the proper handling of government records according to the orders, policies, and regulations which govern them.

e) I will not release such information unless specifically authorized to do so, or as required, on a "need-to-know" basis, in the proper discharge of official duties.

f) I will not divulge any official information obtained through or in connection with my government employment to any unauthorized person or organization.

g) I will not use, or permit others to use, any official information that is not available to the general public for private purposes.

h) I will not remove official documents or records from files for personal or inappropriate reasons. Falsification, concealment, mutilation, or unauthorized removal of official documents or records, either hard copy or electronic, is prohibited.

i) I will not disclose any PII or information contained in Privacy Act records, unless explicitly authorized and in compliance with DOT obligations under the Freedom of Information Act, the Privacy Act, or other federal law.

j) I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I step away from my work area, even for a short time; I will log off or shut my workstation or laptop computer down when I leave for the day.

k) I will properly dispose of DOT sensitive information, either in hardcopy, softcopy or electronic media formats (CD, DVD, USB sticks) in accordance with DOT policy and procedures.

l) I will not access, process, or store classified information on DOT office equipment that has not been authorized for such access, processing or storage.

4 4 Use of Government Office Equipment

a) I understand that DOT and its Components may publish additional Acceptable Use policies to which I must comply.

b) I understand that DOT office equipment is to be used for official use, with only incidental personal use permitted.

c) I understand that my use of DOT office equipment may be monitored, and I consent to this monitoring.

d) I understand that the viewing of pornographic or other offensive or graphic content is strictly prohibited on DOT furnished equipment and networks, unless explicitly approved by Secretarial Office Head or Component Administrator in order to support official duties.

e) I agree to comply with all software copyrights and licenses.

f) I will not download or attempt to install unauthorized software programs on DOT office equipment.

g) I will not install unauthorized software (including software available for downloading from the Internet, software available on DOT networks, and personally owned software) on DOT equipment (e.g., DOT workstations, laptop computers, PEDs).

5 Internet and E-mail Use

a) I understand that Internet activities that may impact the confidentiality, integrity or availability of DOT information and information systems, or cause degradation of network services, are prohibited unless otherwise permitted for official duties. Examples of such activities include streaming of audio or video, peer-to-peer networking, and attempted unauthorized access to DOT or other organizations information systems.

b) I understand that I must use internet web-based technologies such as social media/networking, blogging and messaging, as outlined in DOT Order 1351.33, Appendix A: Employee Conduct Policy.

c) I understand that DOT-provided internet and e-mail is for official use, with incidental personal use allowed.

d) I will not auto-forward e-mail messages on my DOT system to addresses outside the DOT network.

e) I understand that the use and access to internet webmail such as Yahoo, Google and MSN or access to other personal email accounts from DOT information systems is permitted to the extent that it constitutes no more than incidental personal use.

f) I will not host, set up, administer, or operate any type of internet server on any DOT network or attempt to connect any personal equipment to a DOT network unless explicitly authorized in writing by my Component CIO and I will ensure that all such activity is in compliance with DOT security policies.

g) I will not use peer-to-peer (P2P) file sharing to connect remotely to other systems for the purpose of sharing files. I understand that P2P can be a means of spreading viruses over DOT networks and may put sensitive government information at risk. I also understand that DOT Order 1351.37 Department Cybersecurity Policy through its Cybersecurity Compendium prohibits the use of P2P software on any DOT-owned, controlled or operated equipment.

h) I will not provide personal or official DOT information solicited by e-mail. I will be on alert if I receive e-mail from any source requesting personal or organizational information. If I receive an e-mail message from any source requesting personal information or asking to verify accounts or security settings, I will forward the message to the appropriate DOT Help Desk and delete the message from my system.

6 Telecommuting (Working at Home or at a Satellite Center)

Employees approved for telecommuting must adhere to the following rules of behavior:

a) I will comply with DOT Telework Policy DOT Order 1501.1A.

b) At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.

c) I will protect sensitive data at my alternate workplace. DOT Telework Policy specifies guidelines for “Safekeeping of Government Materials/Documents/Equipment.” DOT Telework Policy also requires that all Sensitive Personally Identifiable Information (SPII) only be used when computing media/storage is encrypted with DOT-approved encryption solutions.

7 Laptop Computers and Portable Electronic Devices (PED)

Rules of behavior that specifically apply to DOT laptop computers and portable electronic devices (PEDs) are listed below.

a) I will only use DOT-issued devices (workstations, laptops or PEDs) to access DOT systems and process DOT information.

b) I will password-protect any BlackBerry device, iPhone, or other PED that I use to process DOT information. I will set the security timeout feature to the DOT-specified timeout period so that the device automatically locks and requires a password to unlock. Assistance can be obtained through the appropriate DOT Help Desk.

c) I will keep the laptop or PED under my physical control at all times, or I will secure it in a suitable locked container under my control.

d) I will take all necessary precautions to protect any laptop/PED in my charge against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and when possible encrypted removable media.

e) I will keep antivirus and firewall software installed and up to date on any computer system/laptop in my charge.

f) I will use only DOT-authorized internet connections that conform to DOT security and communications standards.

g) I will not make any changes to the system configuration of any laptop/PED in my charge unless I am directed to do so by a DOT system administrator.

h) I will not program any laptop/PED in my charge with sign-on sequences, passwords, or access phone numbers.

i) I agree that I will not have both a DOT network connection and any kind of non-DOT network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my Component CIO.

j) I understand and will comply with the requirement that sensitive information stored on any laptop computer, PED or mobile media such as USB drives and CD/DVDs used outside of DOT-protected facilities must be encrypted using DOT-approved methods.

k) I understand and will comply with the requirement that sensitive information transmitted from wireless devices must be encrypted using DOT approved encryption methods.

l) I understand that the use of Bluetooth and other wireless communications is restricted on DOT information systems and that I must obtain permission for its use from the Component CIO.

8 Travel with Laptop Computers and Portable Electronic Devices

Rules of behavior that specifically apply to traveling with DOT laptop computers and PEDs are listed below.

a) I will keep the laptop or PED in my charge under my physical control at all times.

b) At airport security, I will place any laptop or PED in my charge on the conveyor belt only after the belongings of the person ahead of me have cleared the scanner. If delayed, I will keep my eye on the laptop or PED until I can pick it up.

c) I will not place any laptop or PED in my charge in checked luggage.

d) I will not store any laptop or PED in my charge in an airport, a train or bus station, or other public locker.

e) If I must leave any DOT laptop or PED in my charge in a car, I will lock it in the trunk so that it is out of sight.

f) I will avoid leaving any DOT laptop or PED in my charge in a hotel room. If I must leave it in a hotel room, I will lock it inside a safe provided by the hotel if available.

g) I will obtain written approval from the DOT CISO before taking DOT-issued laptop or PED on foreign (non-US) travel.

9 Incident Reporting

a) I will immediately report suspected or actual IT security incidents or privacy breaches to the DOT's Computer Security Incident Response Center, the FAA Computer Security Management Center (CSMC).

DOT CSMC Phone: 1-866-580-1852, Option 1

DOT CSMC Email: CSMC@dot.gov

b) I will follow the instructions provided by the DOT CSIRC or my DOT Component Information Systems Security Officer (ISSO) or Information Systems Security Manager (ISSM) to support investigation of the incident.

c) I will immediately report suspected or actual privacy breaches to my DOT Component Privacy Officer.

10 Accountability and Personal Liability

I understand that I will be held accountable for my actions while accessing and using DOT systems and IT resources. I am aware that federal law provides for punishment consisting of a fine under Title 18, U.S. Code and up to 10 years in jail for the first offense for anyone who:

a) Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure. (Note that the offense is for the access, and not necessarily any disclosure); or

b) Intentionally accesses a Government information system without authorization and, in so doing, affects the use of the Government's operation of that system; or

c) Intentionally accesses a Government information system without authorization, and alters, damages, or destroys information or prevents authorized use of the system; or

d) Accesses a Government information system without authorization, or exceeds authorized access, and obtains anything of value.

11 Acknowledgment Statement

I understand that failure to comply with these Rules of Behavior could result in oral or written warning, suspension and/or removal of system access, reassignment to other duties, criminal or civil prosecution, or suspension from duty and/or termination of employment, or removal from a contract for contractor personnel. Consequences of failure to comply will be commensurate with the individual's level of responsibility and the nature of the violation.

Additionally, willful unauthorized disclosure of DOT sensitive information, including PII, may result in legal liability for the offender. Individuals who demonstrate egregious disregard or a pattern of failing to comply with the above requirements will have their authority to access information systems promptly revoked.

I understand that I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific DOT systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

By signing this agreement, I understand and consent to the following when I access DOT's information system.

- I acknowledge that I have received a copy of these Rules of Behavior;
- understand, accept and agree to comply with all terms and conditions of these Rules of Behavior;
- I am accessing a U.S. Government information system that is provided for U.S. Government authorized use only;
- The Government, acting directly or through its contractors, routinely monitors communications occurring on this information system. I have no reasonable expectation of privacy regarding any communications or data transiting the Government network or stored on or travelling to its computer systems or storage media. At any time, the government may for any lawful purpose monitor, intercept,

search, and seize any communication or data transiting, stored or traveling to or from this information system; and

- Any communications or data transiting, stored on or traveling to or from this information systems or storage media may be disclosed or used for any lawful government purpose.

DOT's information systems consist of: 1) my desktop computer or laptop; 2) DOT computer networks; 3) all computers connected to DOT networks; and 4) all personal electronic devices (e.g., BlackBerry, iPhone, iPads, PED) and storage media (e.g., thumb drives, flash drives) attached to DOT networks or its computers. By clicking the button below I acknowledge that I understand and consent to these Rules of Behavior.